第 43 卷 第 4 期/2023 年 2 月/光学学报 研究论文

光学学报

基于联合干扰的室内可见光通信安全系统

万子文，吴雅婷*，梁如斌，张倩武

上海大学特种光纤与光接入网重点实验室，特种光纤与先进通信国际合作联合实验室，上海 200444

摘要 研究了典型室内办公场景下，多用户多输入单输出(MISO)可见光通信(VLC)系统的物理层安全问题。针对未知数量的窃听者有可能出现在公共区域内任意位置的场景，提出了一种基于联合干扰的人工噪声生成方案以提高系统的保密安全性能。该方案利用用户所在区域的发光二极管(LED)作为信号源的同时，联合窃听者所在区域的LED一起发送干扰信号。由于窃听者位置随机且未知，故所提方案以最小化最坏情况下窃听者的信干噪比(SINR)为目标，通过干扰形成器的协作优化与设计使得干扰信号在不影响合法用户信号正常接收的前提下，最大程度地扰乱窃听者的接收。仿真结果表明，与传统的人工噪声方案相比，所提的联合干扰策略能明显降低窃听者的信干噪比和提高系统的保密速率，从而使得VLC系统的安全性能得到显著提升。

关键词 光通信；物理层安全；人工噪声；保密速率

中图分类号 TN929.12 **文献标志码** A **DOI**：10.3788/AOS221530

1 引 言

可见光通信(VLC)利用发光二极管(LED)来实现信号的高速传输，兼顾照明和通信功能，具有频谱资源丰富、抗电磁干扰和成本低等优点，近年来受到了广泛关注[1-4]。光线具有开放式的广播特性，这意味着当可见光系统的通信节点部署在开放空间中时，潜在的窃听者可以接收到传输给合法用户的机密信号[5]。在众多的安全方法中，物理层安全(PLS)技术[6]利用信道特性来隐藏信息，不依赖于上层的加密技术，能有效增强系统的安全性。

近年来许多学者对VLC系统的物理层安全方法进行了深入研究，提出了各种物理层安全技术，如波束形成[7-9]、人工噪声(AN)[10-17]等。文献[7]在窃听者的信道状态信息(CSI)完全已知的理想情况下，采用迫零波束形成将机密信号映射到窃听者CSI的零空间内，使得窃听者接收不到此信号。然而，现实场景中窃听者的CSI通常难以获得，这是VLC安全性研究的难点。文献[8]针对此情况设计了一种鲁棒波束形成方法来提高最坏情况下的保密速率，但此方案对系统安全性的提升有限。

由于人工噪声可在不影响合法用户接收信号的同时干扰窃听者的接收，故其成为了保障VLC系统安全的重要手段[10]。通常采用友好干扰[11]和基于人工噪声的预编码[12]这两种方案来生成人工噪声。在友好干扰方案中，一组LED用来发送机密信号给合法用户，另一组LED负责发送人工噪声。基于人工噪声的预编码方案则利用所有的LED同时发送机密信号和人工噪声。文献[13]在单个窃听者的位置未知时，提出了一种空间干扰方案来生成人工噪声，以提高系统的保密性能，但没有考虑多个窃听者的情形。文献[14]在具有固定位置的多个窃听者情况下，采用基于人工噪声的预编码方案来最大化用户的信干噪比(SINR)。当多个窃听者的位置未知时，文献[15]利用基于人工噪声的预编码方案来最小化系统的发射功率。以上研究[13-15]都是基于单个合法用户的场景，在存在多个合法用户的场景下，文献[16]分别在单个窃听者的位置已知和未知时，采用迫零预编码和人工噪声来提高系统保密速率的总和。在相同的场景下，文献[17]采用基于人工噪声的预编码方案来最大化用户的信干噪比，没有考虑多个具有随机位置的窃听者存在的情景。

在本文中，假设多个合法用户位于办公区域，而随机数目的窃听者有可能出现在公共区域的任意位置，此类场景通常出现在典型的办公场景中，如政府办事处、银行的服务型窗口等。针对这种分区域的情况，本文提出了一种联合干扰策略来提高VLC系统的安全性能。此方案利用办公区域的多个LED光源发送合法用户所需的机密信号，同时联合公共区域的LED一起发送针对窃听者的干扰信号。通过协作设计两个区域的干扰形成器，使得这组联合干扰信号对合法用户

收稿日期：2022-07-26；**修回日期**：2022-08-21；**录用日期**：2022-09-13；**网络首发日期**：2022-09-23

基金项目：上海市科委重点项目(20511102400)、上海市自然科学基金(20ZR1420900)、高等学校学科创新引智计划(D20031)

通信作者：*ytwu@shu.edu.cn

的影响抵消为零。同时，在此基础上建立优化问题，在保证合法用户通信质量的同时，最小化最坏情况下窃听者的信干噪比，从而提高系统保密速率的总和。

2　系统模型

2.1　可见光信道模型

图 1 为室内多用户多输入单输出（MISO）VLC 安全系统模型。在办公区域和公共区域的天花板上分别有 N_A 和 $N-N_A$ 个 LED 光源，每个 LED 均可同时提供照明和通信服务。其中，K 个合法用户（Bob）位于办公区域侧，M 个窃听者（Eve）随机出现在另一侧的公共区域。假设合法用户和窃听者位于同一个水平面上，他们可以通过各自配备的光电二极管（PD）接收到 LED 的发射信号，LED 垂直向下部署，PD 垂直向上面向天花板。

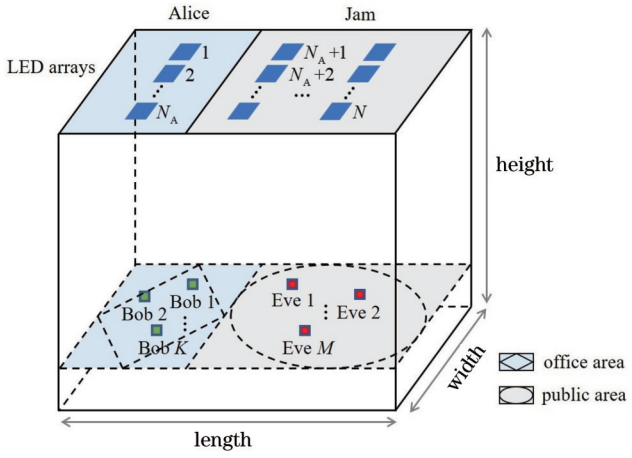

图 1　室内多用户 MISO VLC 安全系统模型

Fig. 1　Indoor multi-user MISO VLC security system model

在室内场景中，由于视距分量的信号强度远高于非视距分量[18-19]，故几乎所有 VLC 安全系统的工作都只考虑了视距链路。本文采用视距链路模型来表征室内 VLC 信道的响应特性，发射端的第 n 个 LED 与接收端的第 i 个 PD 之间的信道增益[19]为

$$h_{n,i}=\eta\zeta\frac{(m+1)S_{\mathrm{PD}}}{2\pi d^2}\cos^m\varphi T(\psi)g(\psi)\cos\psi,\quad(1)$$

式中：η 是 LED 的光电转换率；ζ 为接收端 PD 的响应度；d 为 LED 到 PD 的直线距离；S_{PD} 为 PD 的有效接收面积；$m=-\ln 2/\ln(\cos\theta_{1/2})$ 为表征光源辐射方向性的辐射模式指数，其中 $\theta_{1/2}$ 是光源的半功率角；φ 为 LED 的发射角；ψ 为 PD 的入射角；$T(\psi)$ 为光学滤光片的增益；$g(\psi)$ 为光学集中器的增益。$g(\psi)$ 的表达式[19]为

$$g(\psi)=\begin{cases}\dfrac{\kappa^2}{\sin^2\psi_{\mathrm{FOV}}}, & 0\leqslant\psi\leqslant\psi_{\mathrm{FOV}}\\ 0, & \psi>\psi_{\mathrm{FOV}}\end{cases},\quad(2)$$

式中：κ 为折射系数；ψ_{FOV} 为接收端 PD 的视场角。

2.2　联合干扰方案及优化问题

基于以上信道模型，提出了一种联合干扰方案来为系统提供更高等级的安全性，如图 2 所示。办公区域的 LED（Alice）负责发送机密信号给合法用户，同时联合公共区域的 LED（Jam）一起发送干扰信号。通过设计发射端 Alice 和 Jam 的干扰形成器，使得两者发出的干扰信号对各个用户的干扰相互抵消为零，从而在不影响合法用户的通信质量的同时，最大程度干扰窃听者的接收信号。

具体地，办公区域的 LED 发送给合法用户的机密数据为 $\boldsymbol{u}=[u_1\ u_2\ \cdots\ u_K]^{\mathrm{T}}$，$k=1,2,\cdots,K$，其中 u_k 是发送给第 k 个用户的数据符号。发射端 Alice 和 Jam 联合发送的干扰数据为 s。在不失一般性的前提下，假设发送数据 u_k 和 s 的均值为 0，方差为 $\sigma_{\mathrm{U}}^2=\sigma_{\mathrm{S}}^2$，取值区间为 $[-1,1]$。机密信号 u_k 的预编码器为 $\boldsymbol{w}_k=[w_{1,k}\ w_{2,k}\ \cdots\ w_{N_A,k}]^{\mathrm{T}}$，其中 $|w_{n,k}|\leqslant 1$，$n=1,2,\cdots,N_A$。发射端 Alice 和 Jam 的干扰形成器分别为 $\boldsymbol{v}_A$ 和 $\boldsymbol{v}_J$。

发射端 Alice 和 Jam 的发送信号分别为

$$\begin{cases}\boldsymbol{x}_A=\alpha_1\left[\dfrac{\rho}{K}\displaystyle\sum_{k=1}^{K}\boldsymbol{w}_k u_k+(1-\rho)\boldsymbol{v}_A s\right]+I_D\boldsymbol{1}_{N_A}\\ \boldsymbol{x}_J=\alpha_2\boldsymbol{v}_J s+I_D\boldsymbol{1}_{N-N_A}\end{cases},\quad(3)$$

式中：$\rho\in[0,1]$ 为光功率系数；I_D 为满足 LED 幅值限制而设置的直流偏置（DC-bias）；$\boldsymbol{1}_{N_A}$ 和 $\boldsymbol{1}_{N-N_A}$ 为元素全为 1 的向量；α_1 和 α_2 为幅值系数，需要满足 LED 的幅值限制条件。典型的 LED 受到非线性失真的影响，在其有限的动态范围 $[I_{\min},I_{\max}]$ 内，可以利用预失真进行线性化。直流偏置为 $I_D=(I_{\min}+I_{\max})/2$，最大信号幅值为 $A_m=(I_{\max}-I_{\min})/2$。要使 LED 工作在线性区间，发送信号需满足

$$\begin{cases}\alpha_1\left[\dfrac{\rho}{K}\left\|\displaystyle\sum_{k=1}^{K}|\boldsymbol{w}_k|\right\|_\infty+(1-\rho)\|\boldsymbol{v}_A\|_\infty\right]\leqslant A_m\\ \alpha_2\|\boldsymbol{v}_J\|_\infty\leqslant A_m\end{cases}。\quad(4)$$

接收端 PD 直接检测得到的信号经过交流耦合去除直流后，位于办公区域的第 k 个合法用户的接收信号为

$$y_{B,k}=\boldsymbol{h}_{AB,k}^{\mathrm{T}}\boldsymbol{x}_A+\boldsymbol{h}_{JB,k}^{\mathrm{T}}\boldsymbol{x}_J+n_{B,k}=$$
$$\alpha_1\frac{\rho}{K}\left(\boldsymbol{h}_{AB,k}^{\mathrm{T}}\boldsymbol{w}_k u_k+\boldsymbol{h}_{AB,k}^{\mathrm{T}}\sum_{i=1,i\neq k}^{K}\boldsymbol{w}_i u_i\right)+\alpha_1(1-\rho)\boldsymbol{h}_{AB,k}^{\mathrm{T}}\boldsymbol{v}_A s+\alpha_2\boldsymbol{h}_{JB,k}^{\mathrm{T}}\boldsymbol{v}_J s+n_{B,k},\quad(5)$$

式中：$\boldsymbol{h}_{AB,k}$ 为办公区域的 LED 到第 k 个合法用户的信道增益向量；$\boldsymbol{h}_{JB,k}$ 为公共区域的 LED 到第 k 个合法用户的信道增益向量；$n_{B,k}$ 为平均功率为 σ_N^2 的加性高斯白噪声。第 m 个窃听者的接收信号为

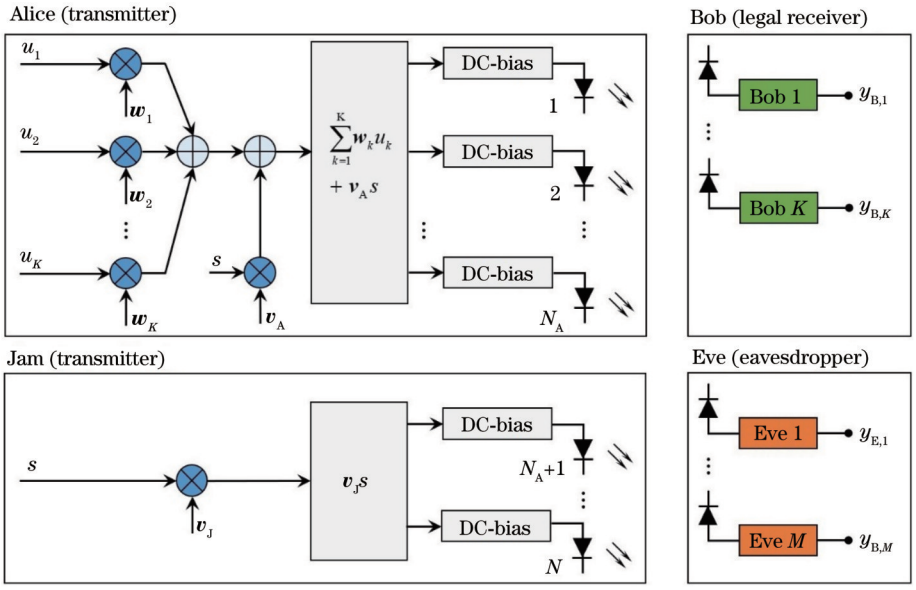

图 2　所提的基于联合干扰的VLC安全方案

Fig. 2　Proposed VLC security scheme based on cooperative jamming

$$y_{\mathrm{E},m}=\boldsymbol{h}_{\mathrm{AE},m}^{\mathrm{T}}\boldsymbol{x}_{\mathrm{A}}+\boldsymbol{h}_{\mathrm{JE},m}^{\mathrm{T}}\boldsymbol{x}_{\mathrm{J}}+n_{\mathrm{E}}=$$
$$\alpha_1\frac{\rho}{K}\left(\boldsymbol{h}_{\mathrm{AE},m}^{\mathrm{T}}\boldsymbol{w}_k u_k+\boldsymbol{h}_{\mathrm{AE},m}^{\mathrm{T}}\sum_{i=1,i\neq k}^{K}\boldsymbol{w}_i u_i\right)+\alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{AE},m}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A}}s+\alpha_2\boldsymbol{h}_{\mathrm{JE},m}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}s+n_{\mathrm{E}},\tag{6}$$

式中：$\boldsymbol{h}_{\mathrm{AE},m}$是办公区域的LED到第$m$个窃听者的信道增益向量；$\boldsymbol{h}_{\mathrm{JE},m}$为公共区域的LED到第$m$个窃听者的信道增益向量；$n_{\mathrm{E}}$为平均功率为$\sigma_{\mathrm{N}}^2$的加性高斯白噪声。

由于窃听者随机分布在公共区域内，故办公区域和公共区域的LED发射源到窃听者的信道特性都无法准确估计。在窃听者的位置随机且不确定的条件下，取$\boldsymbol{w}_k=\boldsymbol{h}_{\mathrm{AB},k}\big/\left\|\boldsymbol{h}_{\mathrm{AB},k}\right\|_2$，这可使得在第$k$个合法用户的接收信号中数据符号$u_k$的信号强度达到最大。同时，为使得发射端Alice和Jam各自发送的干扰信号对第k个合法用户的影响互相抵消，干扰形成器$\boldsymbol{v}_{\mathrm{A}}$和$\boldsymbol{v}_{\mathrm{J}}$应满足限制条件

$$\alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{AB},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A}}+\alpha_2\boldsymbol{h}_{\mathrm{JB},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}=0,\tag{7}$$

此时第k个合法用户接收的信号为

$$y_{\mathrm{B},k}=\alpha_1\frac{\rho}{K}\boldsymbol{h}_{\mathrm{AB},k}^{\mathrm{T}}\boldsymbol{w}_k u_k+\alpha_1\frac{\rho}{K}\boldsymbol{h}_{\mathrm{AB},k}^{\mathrm{T}}\sum_{i=1,i\neq k}^{K}\boldsymbol{w}_i u_i+n_{\mathrm{B},k},\tag{8}$$

第k个合法用户接收的信号的信干噪比为

$$\gamma_{\mathrm{B},k}=\frac{\sigma_{\mathrm{U}}^2\lambda^2\left|\boldsymbol{h}_{\mathrm{AB},k}^{\mathrm{T}}\boldsymbol{w}_k\right|^2}{\sigma_{\mathrm{U}}^2\lambda^2\sum_{i=1,i\neq k}^{K}\left|\boldsymbol{h}_{\mathrm{AB},k}^{\mathrm{T}}\boldsymbol{w}_i\right|^2+\sigma_{\mathrm{N}}^2},\tag{9}$$

式中：$\lambda=\alpha_1\rho/K$。可以看到，满足式(7)的联合干扰信号对第k个合法用户的干扰为零，同时数据符号u_k的信号强度达到最大。在此基础上，最大程度干扰窃听者的接收信号表现为最小化窃听者的信干噪比。对于发送给k个用户的机密数据u_k，第m个窃听者接收信号的信干噪比为

$$\gamma_{\mathrm{E},m,k}=\frac{\sigma_{\mathrm{U}}^2\lambda^2\left|\boldsymbol{h}_{\mathrm{AE},m}^{\mathrm{T}}\boldsymbol{w}_k\right|^2}{\sigma_{\mathrm{U}}^2\lambda^2\sum_{i=1,i\neq k}^{K}\left|\boldsymbol{h}_{\mathrm{AE},m}^{\mathrm{T}}\boldsymbol{w}_i\right|^2+\sigma_{\mathrm{S}}^2\alpha_1^2(1-\rho)^2\left|\boldsymbol{h}_{\mathrm{AE},m}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A}}\right|^2+\sigma_{\mathrm{S}}^2\alpha_2^2\left|\boldsymbol{h}_{\mathrm{JE},m}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}\right|^2+\sigma_{\mathrm{N}}^2}。\tag{10}$$

由于$\gamma_{\mathrm{E},m,k}$随着窃听者位置的变化而改变，且窃听者可能随机出现在公共区域中的任意位置，故为保障最坏情况下系统的安全性能，以最小化最坏情况下窃听者的信干噪比为目标函数建立优化问题，有

$$\underset{\boldsymbol{v}_{\mathrm{A}},\boldsymbol{v}_{\mathrm{J}}}{\text{minimize}}\ \max_{m,k}\left(\gamma_{\mathrm{E},m,k}\right),\ \text{subject to}\begin{cases}\alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{AB},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A}}+\alpha_2\boldsymbol{h}_{\mathrm{JB},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}=0,\ k=1,2,\cdots,K\\ \alpha_1\left[\dfrac{\rho}{K}\left\|\sum_{k=1}^{K}|\boldsymbol{w}_k|\right\|_\infty+(1-\rho)\left\|\boldsymbol{v}_{\mathrm{A}}\right\|_\infty\right]\leqslant A_{\mathrm{m}}\\ \alpha_2\left\|\boldsymbol{v}_{\mathrm{J}}\right\|_\infty\leqslant A_{\mathrm{m}}\end{cases},\tag{11}$$

其中$\boldsymbol{v}_{\mathrm{A}}$和$\boldsymbol{v}_{\mathrm{J}}$需满足式(7)的限制条件，发送信号需满足式(4)的限制条件。

3　优化问题的求解

式(11)为典型的最小化最大值问题。针对此优化问题，先对公共区域进行网络离散化处理。在此区域内等间隔取 L 个点作为窃听者的所有可能位置。根据上述信道模型，可以计算出处于第 l 个位置窃听者的 CSI($\boldsymbol{h}_{\mathrm{AE},l}$ 和 $\boldsymbol{h}_{\mathrm{JE},l}$)。通过式(10)所示的窃听者信干噪比的定义可得到位于第 l 个位置窃听者的信干噪比 $\gamma_{\mathrm{E},l,k}$，其中 $l=1,2,\cdots,L$。接着，引入松弛变量 γ_{EX}，其表达式为

$$\gamma_{\mathrm{EX}}=\max_{l,k}\left(\gamma_{\mathrm{E},l,k}\right), \tag{12}$$

待求解的问题式(11)可转化为

$$\underset{\boldsymbol{v}_{\mathrm{A}},\boldsymbol{v}_{\mathrm{J}},\gamma_{\mathrm{EX}}}{\text{minimize}}\ \gamma_{\mathrm{EX}},\ \text{subject to}\begin{cases}\gamma_{\mathrm{E},l,k}\leqslant\gamma_{\mathrm{EX}},\ l=1,2,\cdots,L\ \text{and}\ k=1,2,\cdots,K\\ \alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{AB},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A}}+\alpha_2\boldsymbol{h}_{\mathrm{JB},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}=0,\ k=1,2,\cdots,K\\ \alpha_1\left[\dfrac{\rho}{K}\left\|\sum\limits_{k=1}^{K}\left|\boldsymbol{w}_k\right|\right\|_{\infty}+(1-\rho)\left\|\boldsymbol{v}_{\mathrm{A}}\right\|_{\infty}\right]\leqslant A_{\mathrm{m}}\\ \alpha_2\left\|\boldsymbol{v}_{\mathrm{J}}\right\|_{\infty}\leqslant A_{\mathrm{m}}\end{cases}。 \tag{13}$$

上述问题要求解目标函数的最小值，而第一个约束条件产生了一个非凸集，为求解此类问题，采用了凹凸过程(CCP)[20]来寻找优化问题的局部最优解，再通过迭代找到问题的最优解。将式(13)的第一个约束条件展开为

$$\lambda^2\left|\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{w}_k\right|^2-\left(\lambda^2\sum_{i=1,i\neq k}^{K}\left|\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{w}_i\right|^2-\sigma_{\mathrm{N}}^2/\sigma_{\mathrm{U}}^2\right)\gamma_{\mathrm{EX}}\leqslant\left[\alpha_1^2(1-\rho)^2\left|\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A}}\right|^2+\alpha_2^2\left|\boldsymbol{h}_{\mathrm{JE},l}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}\right|^2\right]\gamma_{\mathrm{EX}}, \tag{14}$$

通过泰勒级数将式(14)中的 $\left|\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A}}\right|^2$ 展开，有

$$\left|\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A}}\right|^2\geqslant\boldsymbol{v}_{\mathrm{A},0}^{\mathrm{T}}\boldsymbol{h}_{\mathrm{AE},l}\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A},0}+2\left(\boldsymbol{h}_{\mathrm{AE},l}\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A},0}\right)^{\mathrm{T}}\left(\boldsymbol{v}_{\mathrm{A}}-\boldsymbol{v}_{\mathrm{A},0}\right), \tag{15}$$

式中：$\boldsymbol{v}_{\mathrm{A},0}$ 为给定的初始可行解。将式(15)代入式(14)中，使用顺序二次规划[21]标准优化算法找到基于此下界的最优解。接下来，将得到的最优解中 $\boldsymbol{v}_{\mathrm{A}}$ 的值传递给为 $\boldsymbol{v}_{\mathrm{A},1}$，并重复相同的过程，直至目标值的改进小于预定义的阈值 ε。该迭代算法的详细步骤如图 3 所示。

4　仿真结果与分析

为验证所提安全方案在室内 VLC 系统中的安全性能，在大小为 5 m × 5 m × 3 m 的室内房间的天花板上共设置了 9 个 LED，其中有 3 个 LED 位于办公区域上方，其余 LED 布置在公共区域，每个 LED 的平均发射功率为 1 W。仿真中假设有 2 个合法用户在办公区域内，未知数量的窃听者随机出现在公共区域内的任

Giving initial feasible points $\boldsymbol{v}_{\mathrm{A},0}$, index $i=0$ and convergence accuracy ε

Repeating

1. Convexify form

$$f_i\left(\boldsymbol{v}_{\mathrm{A}},\boldsymbol{v}_{\mathrm{A},i}\right)=\boldsymbol{v}_{\mathrm{A},i}^{\mathrm{T}}\boldsymbol{h}_{\mathrm{AE},l}\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A},i}+2\left(\boldsymbol{h}_{\mathrm{AE},l}\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A},i}\right)^{\mathrm{T}}\left(\boldsymbol{v}_{\mathrm{A}}-\boldsymbol{v}_{\mathrm{A},i}\right),\ l=1,2,\cdots,L$$

2. Solving convex problem

$$\underset{\boldsymbol{v}_{\mathrm{A}},\boldsymbol{v}_{\mathrm{J}},\gamma_{\mathrm{EX}}}{\text{minimize}}\ \gamma_{\mathrm{EX}},\ \text{subject to}\begin{cases}\lambda^2\left|\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{w}_k\right|^2-\left(\lambda^2\sum_{i=1,i\neq k}^{K}\left|\boldsymbol{h}_{\mathrm{AE},l}^{\mathrm{T}}\boldsymbol{w}_i\right|^2-\sigma_{\mathrm{N}}^2/\sigma_{\mathrm{U}}^2\right)\gamma_{\mathrm{EX}}\leqslant\gamma_{\mathrm{EX}}\times\left[\alpha_1^2(1-\rho)^2 f_i\left(\boldsymbol{v}_{\mathrm{A}},\boldsymbol{v}_{\mathrm{A},i}\right)+\alpha_2^2\left|\boldsymbol{h}_{\mathrm{JE},l}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}\right|^2\right],\ l=1,2,\cdots,L,\ k=1,2,\cdots,K\\ \alpha_1(1-\rho)\boldsymbol{h}_{\mathrm{AB},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{A}}+\alpha_2\boldsymbol{h}_{\mathrm{JB},k}^{\mathrm{T}}\boldsymbol{v}_{\mathrm{J}}=0,\ k=1,2,\cdots,K\\ \dfrac{\rho}{K}\left\|\sum_{k=1}^{K}\left|\boldsymbol{w}_k\right|\right\|_{\infty}+(1-\rho)\left\|\boldsymbol{v}_{\mathrm{A}}\right\|_{\infty}\leqslant A_{\mathrm{m}}/\alpha_1\\ \left\|\boldsymbol{v}_{\mathrm{J}}\right\|_{\infty}\leqslant A_{\mathrm{m}}/\alpha_2\end{cases}$$

setting value of $\boldsymbol{v}_{\mathrm{A},i+1}$ as solution of convex problem

3. Updating iteration $i=i+1$

Until convergence

图 3　CCP 算法的迭代步骤

Fig. 3　Iterative steps of CCP algorithm

意位置。合法用户和窃听者均位于距离地面0.5 m的水平接收平面上。使用以房间角落为原点的笛卡儿坐标系，系统参数如表1所示。

表1　系统参数

Table 1　System parameters

Parameter	Value
Half power angle of LED $\theta_{1/2}$ /(°)	60
Dynamic range of LED $[I_{min}, I_{max}]$/A	[1, 5]
Conversion factor of LED η /(W·A^{-1})	0.4
Active area of PD S_{PD} /cm^2	1
Responsivity of PD ζ /(A·W^{-1})	0.54
Field of view at receiver ψ_{FOV} /(°)	60
Gain of optical filter $T(\psi)$	1
Average noise power σ_N^2 /dBm	−95
Refractive index of lens κ	1.5
Variance of signal σ_U^2	1/3
Optical power coefficient ρ	0.5

图4为室内房间LED的布局图。房间的左侧部分区域为办公区域，右侧为窃听者所在的公共区域。图中的圆形标记表示房间内部署的LED，以1.5 m的间距均匀分布在房间内的天花板上，叉形标记表示2个合法用户的所在位置。公共区域的离散化间隔取0.1 m。

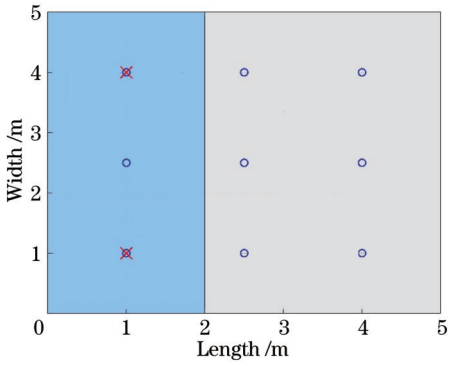

图4　室内LED和用户的位置

Fig. 4　Locations of LEDs and users in room

表2给出了采用不同人工噪声的生成方法时，位于公共区域的窃听者信干噪比的最大值、最小值和均值等统计值。可以看出，采用所提方案时，窃听者信干噪比的最大值、最小值和均值都低于其他两种方法。其中，窃听者信干噪比的最大值是研究的重点，它代表最坏情况下窃听者的信干噪比。在最坏情况下，窃听者的信干噪比为−17.22 dB，分别比采用基于人工噪声的预编码[12]和空间干扰方案[13]低11.73 dB和24.30 dB，这表明在以最小化最坏情况下窃听者的信干噪比为优化目标时，所提方案要优于前两种方案。

表2　不同方案下窃听者的SINR

Table 2　SINR of eavesdroppers in different schemes　　unit: dB

Scheme	Average	Maximum	Minimum	Standard deviation
AN based precoding in Ref. [12]	−16.46	−5.49	−22.33	4.04
Spatial jamming in Ref. [13]	−15.12	7.08	−27.93	9.30
Proposed	−29.10	−17.22	−36.56	5.13

图5显示了采用不同方法生成人工噪声时窃听者的信干噪比。图5(a)、(b)分别对应于发送给第一个或第二个合法用户的机密信号，位于公共区域各个位置窃听者的信干噪比。可以发现，两个子图的数据具有对称性，这是因为两个合法用户和LED的位置关于房间的中轴线对称。以图5(a)为例，当窃听者距离第一

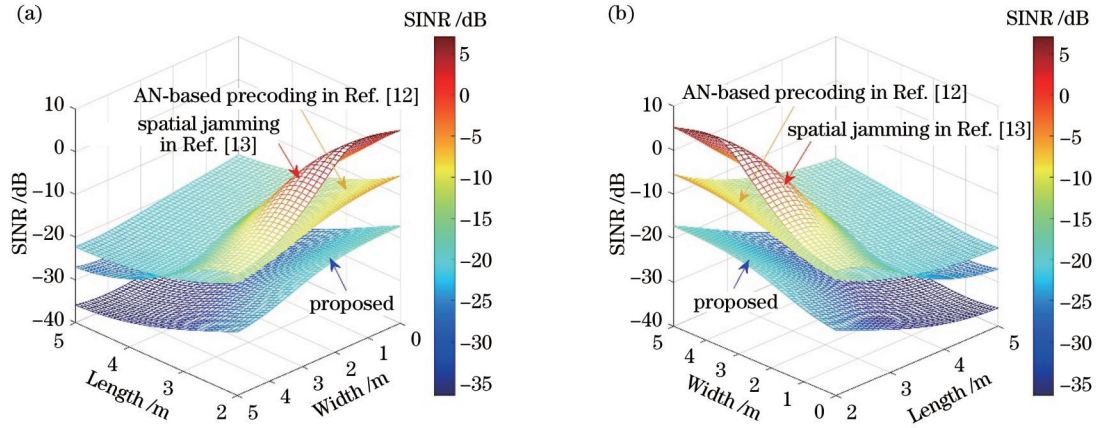

图5　k=1和k=2时不同方案下窃听者的SINR。(a) k=1时窃听者的SINR；(b) k=2时窃听者的SINR

Fig. 5　SINR of eavesdroppers in different schemes at k=1 and k=2. (a) SINR of eavesdroppers at k=1; (b) SINR of eavesdroppers at k=2

个用户越近时，信干噪比数值越大。然而，当窃听者远离此用户时，信干噪比快速下降，最小值相差较大，这是因为在窃听者远离用户时，信号源到窃听者的信道增益衰减，而联合干扰信号对窃听者接收信号的影响不断增加。同时，可以明显地看到，当采用所提的基于联合干扰的人工噪声生成方法时，在整个公共区域内，窃听者的信干噪比要比其他两种方案低，说明经过优化的干扰形成器使得联合干扰信号在不影响合法用户的前提下极大地扰乱了窃听者的接收信号，窃听者很难截获到机密信号。这是因为所提的联合干扰方案产生的干扰信号比基于人工噪声的预编码方案有更大的功率，比空间干扰方案有更大的自由度，进而产生的联合干扰信号的干扰能力更强，系统的保密性能得到了增强。

为定量地衡量系统的安全性能，图 6 给出了当窃听者位于公共区域各个位置时，采用不同方案时系统的保密速率总和的仿真结果。保密速率总和的定义[22]为

$$R_{\mathrm{S}}=\sum_{k=1}^{K}\left[\left(R_{\mathrm{B},k}-R_{\mathrm{E},k}\right)\right]^{+},\tag{16}$$

式中：$[x]^{+}=\max(x,0)$；K为合法用户的个数，$K=2$；$R_{\mathrm{E},k}$是对于发送给第k个合法用户的机密信号，窃听者的可达速率；$R_{\mathrm{B},k}$是第k个合法用户的可达速率。若传输的机密信号在区间$[-1,1]$上均匀分布，可得$R_{\mathrm{E},k}$和$R_{\mathrm{B},k}$的表达式[22]为

$$R_{\mathrm{B},k}=\frac{1}{2}\mathrm{lb}\left(4\lambda^{2}\sum_{i=1}^{K}\left|\boldsymbol{h}_{\mathrm{AB},i}^{\mathrm{T}}\boldsymbol{w}_{k}\right|^{2}+2\pi\mathrm{e}\sigma_{\mathrm{N}}^{2}\right)-\frac{1}{2}\mathrm{lb}\left(\frac{2}{3}\pi\mathrm{e}\lambda^{2}\sum_{i=1,i\neq k}^{K}\left|\boldsymbol{h}_{\mathrm{AB},i}^{\mathrm{T}}\boldsymbol{w}_{k}\right|^{2}+2\pi\mathrm{e}\sigma_{\mathrm{N}}^{2}\right),\tag{17}$$

$$R_{\mathrm{E},k}=\frac{1}{2}\mathrm{lb}\left(1+\gamma_{\mathrm{E},l,k}\right)。\tag{18}$$

从图 6 可以看出，在靠近合法用户一侧的小部分区域中，保密速率总和较低。当窃听者远离合法用户时，系统的保密速率总和较大，这与图 5 反映的结果一致。另外，在窃听者远离合法用户的过程中，系统的保密速率总和的提升逐渐减弱，这是因为当窃听者的信干噪比低于一定数值后，窃听者的可达速率趋近于0，系统的保密速率逐渐收敛于合法用户的可达速率。当采用所提方案时，系统保密速率总和的最小值分别比采用基于人工噪声的预编码和空间干扰方案提高了0.39 bit·s^{-1}·Hz^{-1}和0.78 bit·s^{-1}·Hz^{-1}，这表明在最坏情况下，所提方案在保密性能上优于传统的两种方案。

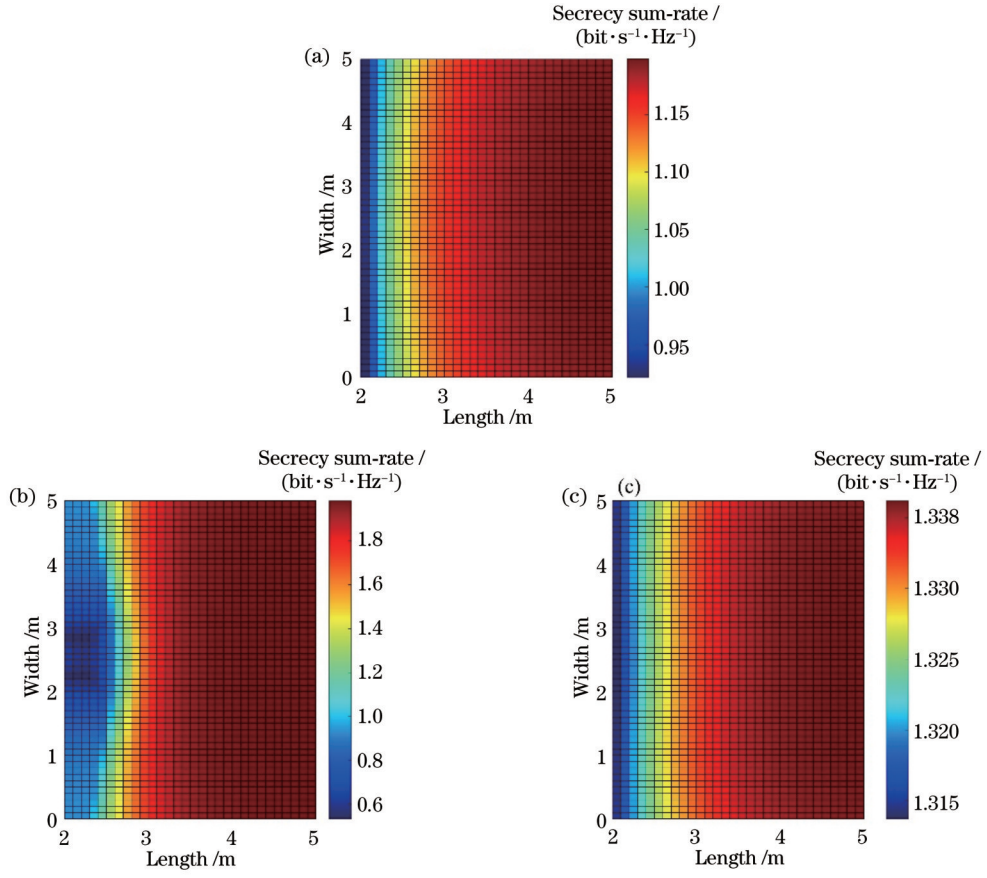

图 6　不同方案下系统的保密速率总和。(a)基于AN的预编码方案；(b)空间干扰方案；(c)所提方案

Fig. 6　System secrecy sum-rate in different schemes. (a) AN-based precoding; (b) spatial jamming; (c) proposed scheme

5 结 论

研究了典型办公场景下多用户MISO VLC系统的物理层安全性问题。当用户和窃听者分别位于不同的区域且窃听者的数目与位置随机不定时,提出了一种联合干扰方法来生成AN。办公区域的LED作为信号源的同时,联合公共区域的LED共同发送干扰信号,通过干扰形成器的联合优化设计使得干扰信号在不影响合法用户的通信质量的同时,最小化最坏情况下窃听者的信干噪比。仿真结果表明,与基于人工噪声的预编码和空间干扰方案相比,所提联合干扰方案在最坏情况下,窃听者的信干噪比分别下降了11.73 dB和24.30 dB。系统的保密速率总和有明显的提高,从而所提方案可有效提升系统的安全性。

参 考 文 献

[1] Arfaoui M A, Soltani M D, Tavakkolnia I, et al. Physical layer security for visible light communication systems: a survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1887-1908.

[2] 亢令川, 王超, 穆昱, 等. 室内多小区可见光通信系统孔径阵列接收机的优化设计[J]. 光学学报, 2021, 41(11): 1106002.
Kang L C, Wang C, Mu Y, et al. Optimal design of aperture array receivers for indoor multicell visible light communication system[J]. Acta Optica Sinica, 2021, 41(11): 1106002.

[3] 贾科军, 魏少博, 蔺莹, 等. 可见光通信预编码光正交频分复用系统的研究[J]. 光学学报, 2021, 41(17): 1706004.
Jia K J, Wei S B, Lin Y, et al. Research on precoding optical orthogonal frequency division multiplexing system in visible light communication[J]. Acta Optica Sinica, 2021, 41(17): 1706004.

[4] 赵黎, 韩中达, 张峰. 基于神经网络的可见光室内立体定位研究[J]. 中国激光, 2021, 48(7): 0706004.
Zhao L, Han Z D, Zhang F. Research on stereo location in visible light room based on neural network[J]. Chinese Journal of Lasers, 2021, 48(7): 0706004.

[5] Li X, Zhang R, Hanzo L. Optimization of visible-light optical wireless systems: network-centric versus user-centric designs[J]. IEEE Communications Surveys & Tutorials, 2018, 20(3): 1878-1904.

[6] Yang N, Wang L F, Geraci G, et al. Safeguarding 5G wireless communication networks using physical layer security[J]. IEEE Communications Magazine, 2015, 53(4): 20-27.

[7] Mostafa A, Lampe L. Physical-layer security for MISO visible light communication channels[J]. IEEE Journal on Selected Areas in Communications, 2015, 33(9): 1806-1818.

[8] Mostafa A, Lampe L. Optimal and robust beamforming for secure transmission in MISO visible-light communication links [J]. IEEE Transactions on Signal Processing, 2016, 64(24): 6501-6516.

[9] Arfaoui M A, Rezki Z, Ghrayeb A, et al. On the input distribution and optimal beamforming for the MISO VLC wiretap channel[C]//2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP), December 7-9, 2016, Washington, DC, USA. New York: IEEE Press, 2016: 970-974.

[10] Mostafa A, Lampe L. Physical-layer security for indoor visible light communications[C]//2014 IEEE International Conference on Communications, June 10-14, 2014, Sydney, NSW, Australia. New York: IEEE Press, 2014: 3342-3347.

[11] Mostafa A, Lampe L. Securing visible light communications via friendly jamming[C]//2014 IEEE Globecom Workshops, December 8-12, 2014, Austin, TX, USA. New York: IEEE Press, 2014: 524-529.

[12] Arfaoui M A, Rezki Z, Ghrayeb A, et al. On the secrecy capacity of MISO visible light communication channels[C]//2016 IEEE Global Communications Conference, December 4-8, 2016, Washington, DC, USA. New York: IEEE Press, 2016.

[13] Cho S, Chen G J, Coon J P. Securing visible light communications with spatial jamming[C]// 2019 IEEE International Conference on Communications, May 20-24, 2019, Shanghai, China. New York: IEEE Press, 2019.

[14] Shen H, Deng Y Q, Xu W, et al. Secrecy-oriented transmitter optimization for visible light communication systems[J]. IEEE Photonics Journal, 2016, 8(5): 7905914.

[15] Pham T V, Pham A T. Energy efficient artificial noise-aided precoding designs for secured visible light communication systems[J]. IEEE Transactions on Wireless Communications, 2021, 20(1): 653-666.

[16] Pham T V, Pham A T. Secrecy sum-rate of multi-user MISO visible light communication systems with confidential messages [J]. Optik, 2017, 151: 65-76.

[17] Pham T V, Hayashi T, Pham A T. Artificial-noise-aided precoding design for multi-user visible light communication channels[J]. IEEE Access, 2018, 7: 3767-3777.

[18] Marshoud H, Muhaidat S, Sofotasios P C, et al. Optical non-orthogonal multiple access for visible light communication[J]. IEEE Wireless Communications, 2018, 25(2): 82-88.

[19] Komine T, Nakagawa M. Fundamental analysis for visible-light communication system using LED lights[J]. IEEE Transactions on Consumer Electronics, 2004, 50(1): 100-107.

[20] Lipp T, Boyd S. Variations and extension of the convex-concave procedure[J]. Optimization and Engineering, 2016, 17 (2): 263-287.

[21] Boggs P T, Tolle J W. Sequential quadratic programming[J]. Acta Numerica, 1995, 4: 1-51.

[22] Ben Y L, Chen M, Cao B H, et al. On secrecy sum-rate of artificial-noise-aided multi-user visible light communication systems[C]//2021 IEEE International Conference on Communications Workshops, June 14-23, 2021, Montreal, QC, Canada. New York: IEEE Press, 2021.

Indoor Visible Light Communication Security Systems Based on Cooperative Jamming

Wan Ziwen, Wu Yating*, Liang Rubin, Zhang Qianwu

Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai 200444, *China*

Abstract

Objective Visible light communication (VLC) has received extensive attention in recent years owing to its numerous advantages such as abundant spectrum resources, immunity to electromagnetic interference, low cost, etc. Due to the inherent broadcast characteristics of VLC, VLC channels are inevitably susceptible to eavesdropping by potential unauthorized users who are inside the same open area illuminated by the light-emitting diode (LED) transmitters. Therefore, security of VLC systems has become an issue of critical importance and substantial efforts have been devoted to it. Among the existing security methods, physical layer security (PLS) schemes have been applied to enhance the overall system security by complementing existing cryptography-based security techniques of upper layers. PLS techniques use channel characteristics and physical-layer features (such as multi-antenna and cooperative nodes) to reduce the attained information at the eavesdroppers. Artificial noise has been emerged as a promising technique to improve the security of multi-user multiple-input multiple-output (MISO) VLC systems. Artificial noise will disturb the eavesdroppers′ reception without affecting the legitimate users′ signals. Most of researches on artificial noise assume a single legitimate user with an eavesdropper of unknown location, and do not consider the realistic scenarios where multiple legitimate users and multiple eavesdroppers with random locations exist. Such scenarios are common in indoor workplaces including government offices, banks, etc. To enhance the security performance under the above typical scenarios, this paper proposes an artificial noise generation scheme based on cooperative jamming to minimize the signal to interference plus noise ratio (SINR) of the eavesdropper in the worst case and improve the security performance of the VLC system.

Methods In a MISO visible light communication system, an artificial noise generation scheme based on cooperative jamming is proposed to improve the security performance of the system when unknown number of eavesdroppers may appear anywhere in the public area. In the proposed scheme, the signal source LEDs in the legitimate user′s area jointly send jamming signals with the LEDs in the public area. Through the joint design of the jammers in the two areas, the effect of the jamming signals on the legitimate user′s reception can be cancelled to zero. On this basis, we formulate an optimization problem to minimize the SINR of the eavesdropper in the worst case, and use the concave-convex process (CCP) to find the optimal solution. Through the joint optimization and design of the jammers, the generated jamming signals will disturb the eavesdropper′s reception to the greatest extent without affecting the legitimate users′ signals, thus enhancing the secrecy sum-rate and security performance of the system.

Results and Discussions To verify the proposed scheme, a typical office scenario is set up for simulation, where 9 LEDs are distributed on the ceiling of an indoor room. 3 LEDs are located above the office area and the rest are arranged in the public area. The average emission power of each LED is 1 W. Without loss of generalization, two legitimate users are assumed in the office area, and an unknown number of eavesdroppers randomly appear anywhere in the public area. Both legitimate users and eavesdroppers are located on a horizontal receiving plane of 0.5 m from the ground. The other parameters are given in Table 1. Simulation results show that the maximum value of the SINR of the eavesdropper in the public area is −17.22 dB when using the proposed cooperative jamming scheme (Table 2), which represents SINR of the eavesdropper in the worst case. Compared with the artificial noise-based precoding and spatial jamming schemes, the SINR of the eavesdropper decreases by 11.73 dB and 24.30 dB in the worst case, respectively (Table 2), and the SINR of the eavesdropper is lower than the traditional two schemes in the whole public area (Fig. 5). At the same time, the minimum value of the secrecy sum-rate of the system is increased by 0.39 bit·s^{-1}·Hz^{-1} and 0.78 bit·s^{-1}·Hz^{-1}, respectively (Fig. 6). This shows that the proposed scheme outperforms the traditional two schemes when the optimization objective is to minimize the eavesdropper′s SINR in the worst case. Through the joint optimization and design, the jamming signals will disturb the eavesdropper′s reception to the maximum extent without affecting the legitimate user′s reception.

Conclusions This paper studies the physical layer security of MISO VLC systems under typical indoor office scenarios. When users and eavesdroppers are located in different areas and the number and location of eavesdroppers are random, a

cooperative jamming method is proposed to generate artificial noise. On one hand, the LEDs in the office area send confidential signals required by legitimate users. On the other hand, the LEDs in the office area jointly send jamming signals with the LEDs in the public area. Through the joint optimization and design of the jammers in different areas, the jamming signals will minimize eavesdropper′s SINR in the worst case without affecting the communication quality of legitimate users. Simulation results show that compared with the artificial noise-based precoding and spatial jamming schemes, the proposed cooperative jamming scheme reduces the eavesdropper′s SINR in the worst case by 11.73 dB and 24.30 dB, respectively. The secrecy sum-rate has been significantly improved, thereby improving the security of the system.

Key words optical communications; physical layer security; artificial noise; secrecy rate